SPN-AS: A new white-box cryptographic algorithm based on AS iteration structure

Ya-tao Yang (yy2008@163.com)
Beijing Electronic Science and Technology Institute
Yu-ying Zhai
Xidian University
Hui Dong
Beijing Electronic Science and Technology Institute

Research Article

Keywords: White-box cryptography, Block cipher, Substitution permutation network structure, Anti-key extraction, Anti-code lifting

Posted Date: March 29th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2737865/v1

Additional Declarations: No competing interests reported.

SPN-AS: A new white-box cryptographic algorithm based on AS iteration structure

Yang Ya-tao[1,2*], Zhai Yu-ying[2†] and Dong Hui[1†]

[1*] Department of Electronic and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China.
[2] School of Telecommunication Engineering, Xidian University, Xi'an 710071, China.

*Corresponding author. E-mail: yy2008@163.com;
Contributing authors: 382207670@qq.com; 804027763@qq.com;
† These authors contributed equally to this work.

Abstract

The attacker in white-box model has full access to software implementation of a cryptographic algorithm and full control over its execution environment. In order to solve the issues of high storage cost and inadequate security about most current white-box cryptographic schemes, SPN-AS, a novel white-box block cipher based on AS iterative structure is proposed. This scheme utilizes the AS iterative structure to construct a lookup table with a five-layer ASASA structure, and the maximum distance separable matrix is used as a linear layer to achieve complete diffusion in a small number of rounds. Attackers can be prevented from recovering the key under black-box model. The length of nonlinear layer S and affine layer A in lookup table is 16 bits, which effectively avoids decomposition attack against the ASASA structure and makes the algorithm possess anti-key extraction security under the white-box model, while SPN-AS possesses weak white-box (32KB, 112)-space hardness to satisfy anti-code lifting security. SPN-AS has provable security and better storage cost than existing schemes, with the same anti-key extraction security and anti-code lifting security, only 128KB of memory space is required in SPN-AS, which is only 14% of SPACE-16 algorithm and 33% of Yoroi-16 algorithm.

Keywords: White-box cryptography; Block cipher; Substitution permutation network structure; Anti-key extraction; Anti-code lifting

1 Introduction

Modern cryptography is widely used in symmetric cryptographic schemes for data encryption and asymmetric cryptographic schemes for digital signatures and key establishment, etc. Most of the above cryptographic schemes are analyzed for security under the black-box attack model, i.e., assuming that the communication endpoint is trusted and the internal state and algorithmic laws of the algorithm are unknown to the adversary. The attacker in the black box model can only access the input and output of the algorithm and does not know the detailed information generated during the execution of the encryption and decryption algorithm, but the black box model is vulnerable to attacks [1]. In the gray-

box attack model, the attacker can not only access information through untrusted channels, but also side channel information such as electromagnetic radiation, current flow, and running time during the encryption and decryption of the algorithm. By analyzing the side channel information, he can effectively obtain part of the algorithm's operation laws of the cryptographic algorithm and thus recover the key by various means. The analysis under the gray box model is also known as Side Channel Anal-ysis (SCA), which can be used to obtain the side channel information statistically through electromagnetic analysis [2] and other means, and then obtain useful key information, etc.

In recent years, Digital Rights Management(DRM), smartphones and cloud services have emerged, and more and more cryptographic algorithms are running in untrusted endpoint environments. At the same time, various attacks have emerged, such as key whitening attacks, entropy attacks, and software static analysis. In 2002, Chow et al [3] introduced the first white-box attack model, in which an attacker has full access to the software implementation of a cryptographic algorithm and full control over its execution environment, and can change the implementation details of the cryptographic algorithm at will, with full visibility of the algorithm's computational process, posing a huge potential threat to data security. How to securely implement cryptographic algorithms and secure keys in the program has become an urgent problem. Therefore, the study of new white-box cryptographic algorithms can effectively guarantee the security of keys in a white-box environment, enabling the cryptographic algorithm cope with a variety of attacks and help data and information security.

An attacker can launch key extraction attack, decomposition attack and code extraction attack under the white-box model[4]. In key extraction attack, the attacker tries to extract the key from the white-box implementation[5]; in decomposition attack, the attacker tries to find a less costly implementation to maintain the exact same functionality as the original version; in code extraction attack, the attacker uses the original cryptographic program as a large valid key for encrypting/decrypting on different devices. White-box ciphers can provide high strength security in the above attack environment. In this paper, we design the SPN-AS white-box block cipher algorithm using a new lookup table theoretical construction, and analyze and compare the security with other white-box cipher schemes to prove the advantages of this scheme.

2 Realated works

In 2002, Chow et al [3] introduced a white-box attack model and designed a white-box AES (Advanced Encryption Standard) algorithm using a set of key-dependent lookup tables. Chow et al. also proposed a white-box implementation of DES (Data Encryption Standard) by interleaving the use of affine transformation and de-linearization techniques[6], whose main design idea was to hide the key by constructing a lookup table. In 2010, Xiao et al [7] improved the white-box AES proposed in the literature [3] by using a 16-bit linear encoding for the obfuscation operation and abandoning the use of nonlinear encoding, which required considerable memory space for the implementation of this scheme as a way to achieve a higher level of security.

In 2009, Xiao et al [8] used the first white-box implementation of the SM4 algorithm (denoted as the Xiao-SM4 white-box scheme) by constructing a lookup table, which transforms each round of the round function operation into the computation of the affine transform as well as the lookup table, and then the output of the lookup table is dissociated. Karroumi et al [9] proposed an alternative white-box

implementation of AES in 2010, which allows the expected security level of the scheme to be increased from 2^{30} to 2^{91} by using an additional set of coefficients obtained from the pairwise representation of AES. In 2014, Luo et al [10] improved on Xiao et al's white-box AES using nonlinear encoding. In 2016, Bai et al [11] proposed a white-box implementation of the SM4 algorithm (denoted as Bai-Wu SM4 white-box scheme) using the same construction of lookup tables. To improve efficiency, the Bai-Wu SM4 white-box scheme uses two types of lookup tables: one to perform output decoding and encoding of new inputs, and the other to compute the wheel function of the standard SM4 algorithm. In 2020, Yao et al [12] proposed a novel white-box implementation of SM4 by first representing the linear transformation of the SM4 algorithm as a matrix, then constructing each round of round functions as four lookup tables with 8-bit inputs and 64-bit outputs, and extracting meaningful 32-bit data after the lookup table using the shift matrix. In 2021, an attack against this scheme was proposed in the literature[13].

Another design idea for white-box ciphers is to design new white-box block cipher algorithms that are secure under the white-box model. Usually this design is based on key-related components, such as S-boxes. A common property of new white-box algorithm designs is incompressibility, also known as weak white-box security or spatial hardness.

In 2014, Biryukov et al [14] designed a strong white-box public key cryptographic scheme, a weak white-box block cryptographic scheme and a black-box block cryptographic scheme based on the ASASA structure (i.e., nonlinear layer S and affine layer A iterative structure). In 2015, Bogdanov et al [15] proposed a dedicated white-box scheme called SPACE for spatially hard ciphers. SPACE reduces the security against key extraction and decomposition attacks under the white-box attack model to the key recovery problem for block ciphers under the black-box attack model; the design idea used is to construct lookup tables from AES by restricting plaintexts and truncating ciphertexts, which makes the attacker cannot recover the key used to generate the lookup table based on the security of AES alone. The concept of (M, Z)-space hardness security was also proposed for evaluating the strength of white-box ciphers against code extraction attacks, which is a generalization of the weak white-box security concept in the literature[14]. In 2016, Bogdanov et al [16] proposed a new efficient white-box block cipher SPNbox, which is designed using a substitution permutation network SPN (Substitution Permutation Network) structure using small block ciphers as key-dependent S-boxes. The SPNbox can provide all important white-box security properties of quantifiable spatial hardness. In 2017, Lin et al [17] designed a white-box cryptographic scheme based on the ASASASA structure. In 2021, Koike et al [18] designed the white-box block cipher Yoroi to improve the security of code extraction attacks against continuous data leakage by updating incompressible tables. Moreover, Yoroi only needs to update the lookup table periodically and does not require updating the key.

For attacks on white-box ciphers, in 2004, Billet et al [19] proposed an attack against the white-box AES scheme in the literature[3], denoted as the BGE attack; the key was successfully recovered by means of combining lookup tables and offsetting nonlinear encoding. In recent years, attacks against the Xiao-SM4 white-box scheme have continued to emerge. In 2013, Lin et al [20] proposed an attack that can recover the key with a time complexity of 247 . In 2018, Pan et al [21] pointed out some complexity bias in the analysis of T. Lin et al. In 2021, Zhang et al [22] proposed an attack against the Xiao-SM4 white-box scheme, and they proposed IVMDA (Intermediate-Values Mean Difference Analysis) based on

Differential Computational Analysis (DCA), and successfully recovered the round key of the Xiao-SM4 white-box scheme. Meanwhile, Zhang et al. proposed an improved scheme that can resist IVMDA by protecting the output of the lookup table with nonlinear encoding. The above scholars have proposed different design schemes and analysis methods in terms of security analysis and performance enhancement of white-box ciphers, but most of them are based on the modification of existing cryptographic algorithms, which are still deficient in terms of security and spatial performance.

The main contributions of this paper are as follows.

(1) A new white-box block cipher algorithm SPN-AS is proposed. Using the AS iterative structure, a lookup table with a five-layer ASASA structure is constructed, and the linear layer uses the MDS (Maximum Distance Separable) matrix. In the black-box model SPN-AS can effectively prevent the attacker from recovering the key. The length of both the nonlinear layer S and the affine layer A in the lookup table is 16 bits, which effectively avoids the decomposition attack against the ASASA structure and makes the algorithm secure against key extraction under the white-box model.

(2) The security of the SPN-AS algorithm is proved. The algorithm possesses weak white-box (32KB, 112)-space hardness and satisfies the anti-code extraction security. Compared with other white-box cryptographic schemes, this scheme occupies less memory space and satisfies the design goals of security and efficiency.

3 Preliminary knowledge

The SPN structure was originally proposed by Shannon and the structure belonged to the same iterative algorithm as the Feistel structure. The cryptographic algorithm of the SPN structure uses two key steps of diffusion and obfuscation for multiplicative iteration, which is constructed as follows[23].

(1) Specify the plaintext grouping and key length, and add the generated subkeys to each iteration of the algorithm's encryption and decryption operations.

(2) The plaintext and the key after the operation are subjected to a dissimilarity operation, and then the substitution and replacement operations are performed respectively. The components of Substitution and Permutation are called S-boxes and P-boxes, respectively. The substitution is a nonlinear operation, while the permutation eliminates the statistical properties of the input plaintext and thus better protects the key information.

(3) The ciphertext is obtained by repeated iterations with different iteration rounds designed.

AES is an SPN type block cipher algorithm with a group length of 128 bits and supports three different key sizes, i.e., 128/192/256 bits, denoted as AES-128, AES-192 or AES-256, respectively. In general, AES consists of R rounds with R+1 128-bit round keys, which are obtained from the AES key using the AES key scheduling algorithm; R depends on the key size, i.e., R=10, 12 or 14 in the case of AES-128, AES-192 or AES-256. The initial and final states are the plaintext and ciphertext of AES, respectively, and an AES state is represented by a 4×4 byte array $[state_{i,j}](0 \le i, j \le 3)$, called the state array.

Each AES round contains the following four operations, in particular, a key addition operation is performed before the start of the first round, and the last round has no column mixing operation.

(1) SubBytes: The AES S-box is applied to each byte of the state. AES uses a fixed S-box, denoted by ***S***, which is a nonlinear bijective mapping from 8 bits to 8 bits. The S-box of AES has a high algebraic count.

(2) ShiftRows: In the case of $0 \le i \le 3$, shift each row i of the state array i bytes to the left. The row indexed by i=0 remains unchanged.

(3) Mixcolumns: It is a linear operation in F_{256}^{16}, specific definition:

$$\begin{pmatrix} state'_{0,j} \\ state'_{1,j} \\ state'_{2,j} \\ state'_{3,j} \end{pmatrix} = \begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} \cdot \begin{pmatrix} state_{0,j} \\ state_{1,j} \\ state_{2,j} \\ state_{3,j} \end{pmatrix} \tag{1}$$

(3) AddRoundKey: It is a XOR orientation of the 128-bit round key and the state array.

Bringer et al [24] used a white-box implementation of the AES algorithm by inserting scrambled terms. The means used is to add scrambling to the original scheme, which makes the algebraic structure more complex and thus much more difficult for an attacker to carry out the attack.

4 Design of SPN-AS

4.1 SPN-AS algorithm lookup table construction

The lookup table in this scheme is denoted as S, which consists of a five-layer ASASA structure, and the specific process of lookup table generation is as follows.

(1) Generate a sufficient number of pseudo-random bits using a key. Specifically, the sequence of pseudo-random bits is generated in counter mode using the block cipher E, encrypted with the master key. CTR_DRBG is chosen as the PRNG (Pseudo Random Number Generator) and AES-CTR as the underlying architecture of CTR_DRBG. For example, in the case of E=AES-128, the key of AES-CTR is set as the 128-bit secret master key of this scheme, and the 128-bit plaintexts 0, 1, ... (as many as possible) are encrypted by encrypting the 128-bit plaintexts 0, 1, ... (as many as possible) to finally generate the desired sequence of pseudo-random bits.

(2) Arrange the pseudo-random bits generated in (1) into a 16×16 matrix and check whether the matrix is invertible. If it is invertible, it is left as an invertible affine transform of the A-layer together with any 16-bit constant, which is denoted as $Q_j (j = 1,2,3)$; if it is not invertible, it is discarded.

(3) The pseudo-random bits generated in (1) are used to generate a 16-bit random permutation using the random permutation generation algorithm[25], denoted as $s_j (j = 1,2)$, as the S-layer in the lookup table.

The generated Q_j and s_j are arranged together to be used as the secret key-related S-box in SPN-AS as follows:

$$S = Q_3 \circ s_2 \circ Q_2 \circ s_1 \circ Q_1 \tag{2}$$

4.2 Specific design of SPN-AS algorithm

SPN-AS uses the SPN structure with MDS matrix as the underlying structure and uses the MDS matrix in the linear layer. The group length of SPN-AS is 128 bits and there are 10 rounds of iterations. The

state of SPN-AS is defined as a vector consisting of 8 elements with 16 bits each: $X=\{X_0,\ldots,X_7\}$. The plaintext X^0 is transformed to the ciphertext X^{10} by a round function operation:

$$X^{10}=(\bigcirc_{i=1}^{10}(\sigma^i\circ\theta\circ\gamma))(X^0) \tag{3}$$

Where i is the number of iteration rounds and $\bigcirc$ denotes the composite of the function. The structure of the wheel function is shown in Figure 1. The encryption algorithm of SPN-AS is shown in Algorithm 1 and the decryption algorithm is shown in Algorithm 2.

Algorithm 1 SPN-AS encryption algorithm

INPUT：128-bit plaintext $X=(X_0,X_1,\ldots,X_7)$

OUTPUT：128-bit ciphertext $Y=(Y_0,Y_1,\ldots,Y_7)$

1：**for** $i=1$ to 10 **do**

2： $Y=(S(X_0),S(X_1),\ldots,S(X_7))$

3： $Y=Y\cdot M_{16}$

4： $Y=Y\oplus(8(i-1)+1,8(i-1)+2,...,8(i-1)+8)$

5：**end for**

6：**return** Y

Algorithm 2 SPN-AS decryption algorithm

OUTPUT：128-bit ciphertext $Y=(Y_0,Y_1,\ldots,Y_7)$

INPUT：128-bit plaintext $X=(X_0,X_1,\ldots,X_7)$

1：**for** $i=10$ to 1 **do**

2： $X=Y\oplus(8(i-1)+1,8(i-1)+2,...,8(i-1)+8)$

3： $X=X\cdot M_{16}^{-1}$

4： $X=(S^{-1}(X_0),\ldots,S^{-1}(X_7))$

5：**end for**

6：**return** X

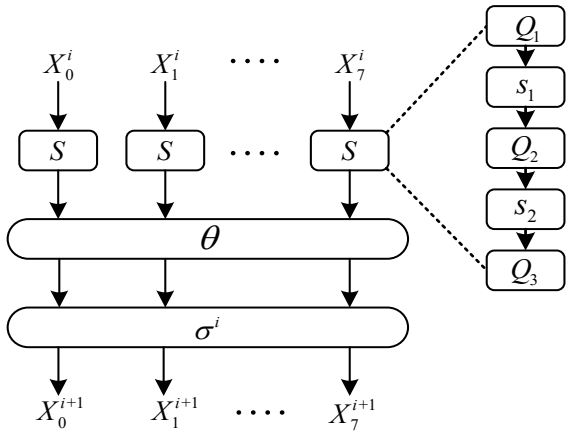

Figure 1 Structure of SPN-AS round function

Each round of SPN-AS contains three layers, which are nonlinear layer γ, linear layer θ, and affine layer σ^i.

(1) Nonlinear layer γ: It is a nonlinear layer constructed from eight secret key-related S-boxes. Since the S-box can be isolated separately by a white-box attacker, it must be an independent primitive that can ensure the n-bit security of the key even if the attacker obtains the complete ciphertext of the S-box. Here, the AS iteration structure is used to generate a lookup table S with a five-layer ASASA structure as the key-related S-box in the nonlinear layer. The nonlinear substitution layer γ is defined as follows.

$$\begin{aligned} &\gamma:(\mathrm{F}_2^{16})^8 \to (\mathrm{F}_2^{16})^8 \\ &(X_0,\ldots,X_7) \mapsto (S(X_0),\ldots,S(X_7)) \end{aligned} \tag{4}$$

(2) Linear layer θ: It is a linear layer that plays a diffusion role. The linear layer θ applies an 8 × 8 MDS matrix with the matrix used in the block cipher [26], defined as follows:

$M_{16} = had(1_x, 3_x, 4_x, 5_x, 6_x, 8_x, \mathrm{b}_x, 7_x)$

Linear layer θ is defined as follows.

$$\begin{aligned} &\theta:(\mathrm{F}_2^{16})^8 \to (\mathrm{F}_2^{16})^8 \\ &(X_0,\ldots,X_7) \mapsto (X_0,\ldots,X_7)\cdot M_{16} \end{aligned} \tag{5}$$

(3) Affine layer σ^i : It is an affine layer, it XOR with C^i which is the constant associated with the round function in round i, defined as follows.

$$\begin{aligned} &\sigma^i:(\mathrm{F}_2^{16})^8 \to (\mathrm{F}_2^{16})^8 \\ &(X_0,\ldots,X_7) \mapsto (X_0 \oplus C_0^i,\ldots,X_7 \oplus C_7^i) \end{aligned} \tag{6}$$

Where $C_j^i = 8(i-1)+j+1$, $0 \le j \le 7$.

5 Security analysis of SPN-AS algorithm

5.1 Security analysis under the black-box model

In the black-box attack model, the attacker's goal is to recover the key. In this case, the attacker attacks by brute-force cracking and its primary goal is to guess the secret component, which in this scenario refers to the lookup table S. The time complexity of the attack here is about $2^{2^{16}\cdot 16}$; if the attacker guesses the master key, the time complexity required here is higher than 2^{128}. Next, the security of SPN-AS under the black-box model is discussed.

(1) Differential cryptanalysis[27]: for differential cryptanalysis, given an input differential a and an output differential b, $a \in \mathrm{F}_2^n$, $b \in \mathrm{F}_2^n$. Then for a function *f*: $\mathrm{F}_2^n \to \mathrm{F}_2^n$, its input is n bits and output is n bits.

The number of differential branches of the linear layer in SPN-AS is 9. Here, assume that the maximum differential probability of the secret S-box in SPN-AS is $2^{-11}(=16/2^{15})$, then the maximum differential probability of the SPN-AS wheel function is 2^{-99}. On the other hand, since the components in the secret S-box are randomly generated and kept secret, it is difficult for an attacker to obtain the actual differential features. SPN-AS has at least 18 active S-boxes after 4 rounds, and if an attacker wants to extend the number of rounds of the differential distinguisher, the increase in the number of rounds

corresponds to the rise in the amount of guessing keys required, and the amount of keys to be guessed for each extended round is $2^{2^{16}\cdot 16}$. From the above analysis, it is clear that 10 rounds of SPN-AS can resist differential cryptanalysis.

(2) Linear cryptanalysis[28]: for linear cryptanalysis, given an input mask α and an output mask β, $\alpha \in \mathrm{F}_2^n$, $\beta \in \mathrm{F}_2^n$. Then for a function *f*: $\mathrm{F}_2^n \to \mathrm{F}_2^n$, whose input is n bits and output is n bits.

The number of linear branches of the linear layer in SPN-AS is 9. Here, assume that the maximum linear probability of the secret S-box in SPN-AS is $2^{-10.62}$. Then the maximum linear probability of the SPN-AS wheel function is $2^{-95.58}$. On the other hand, since the components in the secret S-box are randomly generated and kept secret, it is difficult for an attacker to obtain the actual linear approximation of the round function. SPN-AS has at least 18 active S-boxes after 4 rounds, and if the attacker wants to extend the number of rounds of the linear distinguisher, accordingly, the increase in the number of rounds corresponds to the rise in the amount of required guessing keys, and the amount of keys to be guessed for each extended round is $2^{2^{16}\cdot 16}$. From the above analysis, it is clear that 10 rounds of SPN-AS can resist linear cryptanalysis.

(3) Structural cryptanalysis[29]: structural cryptanalysis usually exploits the propagation properties of a collection of plaintexts with a special structure in the structure of a cryptographic algorithm to initiate an attack. This analysis method generally focuses on the structure of the cryptographic algorithm, independent of the specific algorithmic details, and is therefore particularly suitable for cryptographic algorithms with secret components. A 2.5-round generalized integral distinguisher for SPN-type structures that can recover the secret S-box requires a data complexity of 2^{32} selected plaintexts and a time complexity of 2^{48}. However, no feasible structural cryptanalysis has been found to break a 10-round SPN-AS, so the current 10-round SPN-AS is resistant to structural cryptanalysis.

5.2 Security analysis of anti-key extraction under white-box model

First, a description of the key extraction attack under the white-box model is given.

(1) Decomposition attack on AS iteration structure. The key extraction attack on a white-box block cipher algorithm with AS iterative structure under the white-box model can be reduced to a decomposition attack on the AS iterative structure under the black-box model. Biryukov et al [30] proposed a decomposition attack on the ASASA scheme. It is shown that the decomposition attack on a white-box block cipher algorithm with AS iterative structure holds when the size m of the S-box and the packet length n satisfy the conditions $m^2 \le n$, e.g., 8-bit S-box and 128-bit packet length.

(2) Key recovery attack on the underlying block cipher. The key extraction attack under the white-box model for white-box block ciphers that use the entire codebook of a small block cipher as a lookup table can be reduced to the key recovery attack on the underlying block cipher under the black-box model. The underlying block cipher should be secure against key recovery attacks, i.e., there is no more effective attack than a generic attack such as a brute force attack. For example, the underlying block cipher in SPACE is AES-128, and despite the extensive cryptanalysis work[31][32][33], no effective key recovery attack has been performed so far. More precisely, the key extraction advantage $\mathrm{Adv}_{\mathrm{KE\text{-}WB}}$ of SPACE in

the white-box model , is limited by the key recovery advantage $\mathrm{Adv}_{\mathrm{KR\text{-}BB}}$ of the underlying block cipher in the black-box model: $\mathrm{Adv}_{\mathrm{KE\text{-}WB}} \le \mathrm{Adv}_{\mathrm{KR\text{-}BB}}$.

(3) Key recovery attacks on random permutations. The key extraction attack under the white-box model of the white-box block cipher algorithm that uses random permutations as lookup tables can be reduced to the key recovery attack on random permutations. In this case, a PRNG with some security and a random permutation generation algorithm are used to generate random permutations with each other, e.g., AES-CTR. Although an attacker who knows the complete ciphertext can find the pseudo-random bit string used in the generation by reversing the random permutation generation algorithm, he can only get some plaintext ciphertext pairs of AES-CTR, which cannot be used to recover the key. The security of AES-CTR makes it difficult for an attacker to recover the master key.

In the following, we analyze the security of anti-key extraction under the white-box model.

In the white-box model, an attacker can observe not only the inputs and outputs of the cryptographic algorithm, but also has full access to all entries of the lookup table, i.e., all input-output pairs in the table. For key extraction security, an attacker cannot extract the keys embedded in the white-box scheme. Key extraction attack is the most typical attack strategy against white-box schemes today.

Biryukov et al [30] proposed a decomposition attack on the ASASA scheme. The authors show that the decomposition attack on the ASASA scheme holds when the small S-box, here the size m of the S-box in the nonlinear layer of the ASASA structure and the length n of the block cipher satisfy the conditions $m^2 \le n$, for example, an 8-bit S-box and a 128-bit packet length. As mentioned above, the input and output of the lookup table in SPN-AS with a five-layer ASASA structure are 16 bits, and the S-layer of the lookup table is composed of 16-bit random permutations, and the A-layer is a 16-bit reversible affine transformation, i.e., both m and n are 16 bits, which does not satisfy the condition $m^2 \le n$, so the lookup table in this scheme is secure against such a decomposition attack.

From the above analysis, it is clear that the ASASA structure of the lookup table in this scheme can resist the decomposition attack. Therefore, the attacker cannot recover the A and S layers of the lookup table, and cannot successfully extract the master key K_{AES} of AES-CTR, so it is secure against key extraction.

5.3 Security analysis of anti-code extraction under white-box model

In a mobile payment application scenario, an attacker located in the user's phone, for example, malware may try to extract the decryption key and use it to recover the transaction credentials; or it may copy the entire application to run on the phone of its choice to communicate with the payment terminal of its choice. Therefore, white-box passwords should also have security against code extraction. In this paper, the definition of weak white-box spatial hardness is used to measure the strength of SPN-AS against code extraction attacks.

The group length of SPN-AS is 128 bits, and there are 8 secret S-boxes in the nonlinear layer, each with 16 bits of input and output, for a total of 10 iterations. In order to increase the probability of correctly decrypting a random ciphertext, an attacker can use a space of size less than M to store the explicit ciphertext pairs.

SPN-AS has weak white-box (32KB, 112)-space hardness, which means that even if an attacker succeeds in stealing a quarter of the entire lookup table, he cannot correctly decrypt a randomly selected ciphertext with a probability greater than 2^{-112}.

5.4 Side channel attack analysis

Bos et al [34] proposed a new class of side channel analysis means called DCA. DCA can be considered as a software version of the equivalent of Differential Power Analysis (DPA) applied to hardware. This analysis exploits memory access patterns during the execution of white-box AES software, which allows attackers to execute binaries and simultaneously use dynamic binary tool frameworks such as PIN and Valgrind; by acquiring software traces, they can record read and write access traces to memory. Software traces are used to record the memory addresses accessed by the program during the encryption process. These traces also include other information that can be monitored using binary instrumentation, such as stack reads or register values. Software traces are used to determine which encryption algorithm is implemented, to determine the approximate location of the encryption algorithm in the software implementation, and to perform statistical analysis to extract the secret key. Side channel analysis takes advantage of the fact that each lookup table depends on only a small portion of the key, such as 8 or 16 bits of the key. DCA can efficiently extract a small portion of the key with the help of side channel leakage. However, the lookup table in this scheme contains the full 128 bits of key information. Therefore, even if an attacker can completely monitor the memory access pattern of the target key-related lookup table, the amount of information that the attacker has to guess is 2^{128}. Therefore, SPN-AS is resistant to DCA.

5.5 White-Box Diversity and White-Box Ambiguity Analysis

White-box diversity[3]: refers to the total number of possible lookup tables constructed in a white-box scheme. Therefore, the greater the white-box diversity, the more difficult it is for a cryptanalyst to break the scrambled code, and the more secure the white-box scheme is.

White-box ambiguity[35]: refers to the number of possible constructions for a given white-box cipher or lookup table. The larger the white-box ambiguity, the more difficult it is for the analyst to compute the key disambiguation code and the initial key, and the more secure the scheme is.

The number of integrable matrices of order 16 on F_2 is approximately 2^{254}, thus.

White-Box diversity: $(2^{16\times 2^{16}})^2 \times (2^{16} \times 2^{254})^3$

White-Box Ambiguity: $(2^{16\times 2^{16}}) \times (2^{16} \times 2^{254})^3$.

6 Space Occupancy Analysis and Comparison

The memory space required for SPN-AS is $16 \times 2^{16} = 128\text{KB}$, a comparison with other white-box solutions is shown in Table 1.

Table 1 Comparison of different White-Box schemes

Scheme	Space Occupancy	Anti-key extraction	Anti-code extraction
Whitebox ASASA[14]	8MB	×	×
SPACE-16[15]	918KB	√	√
SPACE-24[15]	218MB	√	√

Whiteblock-16[36]	2MB	√	√
FPL-AES[37]	13.75MB	√	√
WARX[38]	128KB	√	√
Yoroi-16[18]	384KB	√	√
Yoroi-32[18]	48GB	√	√
SPN-AS	128KB	√	√

In the literature [14], the authors used the ASASA structure to construct a white-box cryptographic scheme that occupies 8MB of memory space, but it is currently compromised and cannot resist key extraction attacks as well as code extraction attacks under the white-box model. The SPACE-16 scheme in the literature [15] occupies 918KB of memory space and the SPACE-24 scheme in the literature [15] occupies 218MB of memory space. The SPACE scheme adopts a very conservative design strategy and its internal round function needs to call a full 10 rounds of AES-128, thus it is less efficient. The Whiteblock-16 scheme in the literature [36] occupies 2MB of memory space and achieves incompressibility by using key-dependent pseudorandom functions. The FPL-AES scheme in the literature [37] uses parallel lookup tables to design whiteblock ciphers with high storage cost and requires 13.75MB of storage space. The WARX scheme in literature [38] uses modulo-add, shift, heterogeneous original language and MDS matrix and WARX is more efficient than SPNbox-16 and WEM. The Yoroi-16 scheme in literature [18] enhances the security of code extraction attacks against persistent leaks by updating incompressible tables, but requires multiple lookup tables and 384KB of storage space. The Yoroi-32 scheme in the literature [18] requires a large storage space of 48GB. Compared with other white-box cryptographic algorithms, SPN-AS has a lower storage cost of 128KB and the size of both S and A layers in its lookup table is 16 bits, so it can resist decomposition attacks against ASASA structure, and it has anti-key extraction security and anti-code extraction security under the white-box model.

7 Conclusion

In this paper, we propose a new white-box block cipher algorithm SPN-AS. The design uses the AS iterative structure to construct a lookup table with a five-layer ASASA structure, and uses the SPN structure with MDS matrix as the underlying structure to reduce the number of rounds of the algorithm and improve the implementation efficiency of SPN-AS by taking advantage of the good diffusion property of MDS matrix.

The security analysis shows that SPN-AS can effectively prevent the attacker from recovering the key under the black-box model. Secondly, since the size of both S-layer and A-layer in the lookup table is 16 bits, they can resist the decomposition attack against the ASASA structure, and SPN-AS has anti-key extraction security under the white-box model. Finally, the strength of SPN-AS against code extraction attacks is evaluated using weak white-box space hardness. Compared with other white-box cryptographic algorithms, this scheme takes up less memory space. With the same anti-key extraction security and anti-code extraction security, SPN-AS requires 128KB of memory space, which is only 14% of SPACE-16 and 33% of Yoroi-16, meeting the design goal of security and efficiency, and can be used

for digital rights management, mobile payment, etc. It can be used for information protection in digital rights management, mobile payment, etc.

Declarations

This work was supported by National First-class Under graduate Dicipline Construction of “Communication Engineering” and “Electronic Information Engineering”.

References

[1] Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]. Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1996: 104-113.

[2] Chari S, Rao J R, Rohatgi P. Template attacks[C]. International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2002: 13-28.

[3] Chow S, Eisen P, Johnson H, et al. White-box cryptography and an AES impleme-ntation[C]. International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2002: 250-270.

[4] Chen J, Tong P, Yao S. A white-box implementation of lightweight block cipher GIFT[J]. Information Network Security, 2021, 21(02): 16-23.

[5] Yao S, Chen J, Gong Yating, etc. A new white-box implementa-tion of CLEFIA algorithm[J]. Journal of Xidian University, 2020, 47(05): 150-158.

[6] Chow S, Eisen P, Johnson H, et al. A white-box DES implementa-tion for DRM a-pplications[C]. ACM Workshop on Digital Rights Management. Springer, Berlin, Heidelberg, 2002: 1-15.

[7] Xiao Y. White Box Cryptography and Implementation of AES and SMS4 Algorithms [D]. Shanghai Jiaotong University, 2010.

[8] Xiao Y, Lai X. White Box Cryptography and White Box Imple-mentation of SMS4 Algorithm. 2009 Annual Meeting of Chinese Cryptography Society[M], Beijing: Science Press, 2009: 24-34.

[9] Karroumi M. Protecting white-box AES with dual ciphers[C]. International Conference on Information Security and Cryptology. Springer, Berlin, Heidelberg, 2010: 278-291.

[10] Luo R, Lai X, You R. A new attempt of white-box AES imple-mentation[C]. Proceedings 2014 IEEE International Conference on Security, Pattern Analysis, and Cybernetics. New Jersey, Pis-cataway: IEEE, 2014: 423-429.

[11] Bai K, Wu C. A secure white-box SM4 implementation[J]. Secu-rity and Communication Networks, 2016, 9(10): 996-1006.

[12] Yao Si, Chen Jie. A New White Box Implementation of SM4 Algorithm[J]. Journal of Cryptologic Research, 2020, 7(3): 358-374.

[13] Lu J, Li J. Cryptanalysis of two white-box implementations of the SM4 block cipher[C]. International Conference on Information Security. Cham: Springer International Publishing, 2021: 54-69.

[14] Biryukov A, Bouillaguet C, Khovratovich D. Cryptographic schemes based on the ASASA structure: Black-box, white-box, and public-key[C]. International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2014: 63-84.

[15] Bogdanov A, Isobe T. White-box cryptography revisited: Space-hard ciphers[C]. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2015: 1058-1069.

[16] Bogdanov A, Isobe T, Tischhauser E. Towards practical white-box cryptography: Optimizing efficiency and space hard-ness[C]. International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidel-berg, 2016: 126-158.

[17] Lin T , Lai X , Xue W , et al. A new feistel-type white-box en-cryption scheme[J]. Journal of Computer Science and Technolo-gy, 2017, 32(2): 386-395.

[18] Koike Y, Isobe T. Yoroi: Updatable white-box cryptography[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021, 2021(4): 587-617.

[19] Billet O, Gilbert H, Ech-Chatbi C. Cryptanalysis of a white-box AES impleme-ntation[C]. International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2004: 227-240.

[20] Lin T, Lai X. An Effective Attack on White Box SMS4 Imple-mentation[J]. Journal of Software, 2013, 24(9): 2238-2249.

[21] Pan W, Qin T, Jia Y, et al. Analysis of two SM4 white-box schemes[J]. Journal of Cryptologic Research, 2018, 5(6): 651-671.

[22] Zhang Y, Xu D, Chen J. Analysis and Improvement of White-box SM4 Implementation[J]. Journal of Electronics and Information Technology, 2021, 43: 1-11.

[23] Kong M. Differential Fault Attacks Against Feistel and SPN Cryptographic Structures [D]. Changsha University of Science and Technology, Changsha, 2021.

[24] Bringer J, Chabanne H, Dottax E. White-box cryptography: An-other attempt[J]. IACR Cryptology ePrint Archive, 2006, 2006(51): 468.

[25] Bacher A, Bodini O, Hwang H K, et al. Generating random per-mutations by coin tossing: Classical algorithms, new analysis, and modern implementation[J]. ACM Trans. Algorithms, 2017, 13(2): 24:1-24:43.

[26] Barreto P, Rijmen V. The Khazad legacy-level block cipher[J]. Primitive submitted to NESSIE, 2000, 97(106).

[27] Biham E, Shamir A. Differential cryptanalysis of the data en-cryption standard[M]. Springer Science & Business Media, 2012.

[28] Matsui M. Linear cryptanalysis method for DES cipher[C]. Workshop on the Theory and Application of Cryptographic Tech-niques. Springer, Berlin, Heidelberg, 1993: 386-397.

[29] Biryukov A, Shamir A. Structural cryptanalysis of SASAS[J]. Journal of Cryptology, 2010, 23(4): 505-518.

[30] Biryukov A, Khovratovich D. Decomposition attack on SASASASAS[J]. Cryptology ePrint Archive, 2015, 2015: 646.

[31] Bogdanov A, Khovratovich D, Rechberger C. Biclique crypta-nalysis of the full AES[C]. International Conference on the The-ory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2011: 344-371.

[32] Derbez P, Fouque P A, Jean J. Improved key recovery attacks on reduced-round AES in the single-key setting[C]. Annual Interna-tional Conference on the Theory and Applications of Crypto-graphic Techniques. Springer, Berlin, Heidelberg, 2013: 371-387.

[33] Dunkelman O, Keller N, Shamir A. Improved single-key attacks on 8-round AES-192 and AES-256[C]. International Conference on the Theory and Application of Cryptology and Information Se-curity. Springer, Berlin, Heidelberg, 2010: 158-176.

[34] Bos J, Hubain C, Michiels W, et al. Differential computation analysis: Hiding your white-box designs is not enough[C]. Inter-national Conference on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2016: 215-236.

[35] Xiao Y, Lai X. A secure implementation of white-box AES[C]. 2nd IEEE International Conference on Computer Science and its Applications. Jeju. Korea(South), 2009: 1-6.

[36] Fouque P, Karpman P, Kirchner P, et al. Efficient and provable white-box primitives[C]. International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2016: 159-188.

[37] Kwon J, Lee B, Lee J, et al. FPL: White-box secure block cipher using parallel table look-ups[C]. Cryptographers' Track at the RSA Conference. Cham: Springer International Publishing, 2020: 106-128.

[38] Liu J, Rijmen V, Hu Y, et al. WARX: Efficient white-box block cipher based on ARX primitives and random MDS matrix[J]. Science China Information Sciences, 2022, 65(3): 1-15.